SECFIRM Security Consultants

Unternehmensberatung | Sicherheitsunternehmen | Begutachtung

Der Perimeter im Objektschutz

mgr Mario Trutzenberger EMBA

Sandro M. Trutzenberger B.Sc

Inhalt

Einleitung

Das aus dem Altgriechischen stammende περίμετρος setzt sich aus der Präposition περί (herum) und dem Substantiv μετρος (Maß) zusammen. „Perimeter“ bezeichnet neben dem Umfang einer ebenen geometrischen Figur und einem augenärztlichen Instrument zur Bestimmung des Gesichtsfeldes den Verteidigungsring um ein (militärisches) Objekt.

Der Sprachgebrauch des Objektschutzes meint mit Perimetersicherung den Schutz von Freigeländen.

Allgemeines

Zunächst muss erwähnt werden, dass unter einer lege artis geplanten und errichteten Perimetersicherung – wie im Bereich des gesamten Objektschutzes - ein aufeinander abgestimmter Maßnahmenmix von baulichen, mechanischen, elektronischen, personellen und organisatorischen Maßnahmen zu verstehen ist, wobei die Maßnahmen auf dem Ergebnis einer Security-Risikoanalyse basieren und Stakeholderforderungen berücksichtigen.

Bauliche Maßnahmen im Perimeter beschränken sich nicht ausschließlich auf eine Umfriedung von Freigeländen mit Mauer oder Zaun, sondern gestalten sich stark risiko- und geländeabhängig: so kann ein ungewolltes oder widerrechtliches Eindringen in eine Freifläche beispielsweise landschaftsbaulich erschwert oder unterbunden werden: ist ausreichend Grundfläche vorhanden und ergibt die Risikoanalyse eine Gefährdung durch eindringende Fahrzeuge, können künstliche Geländekupierungen, Verengungen oder Wasser- bzw. Weichbodenflächen (Sumpf), die mit Fahrzeugen schlecht bis nicht zu überwinden sind, gute Dienste leisten, ohne auf den ersten Blick martialisch zu wirken. Üblicher Weise erfolgt der Schutz gegen ungewolltes/rechtswidriges Betreten/Befahren durch Mauern oder Zaunanlagen, die entsprechende Merkmale und Armierungen aufweisen, um – je nach Risiko – einem Eindringen von Fahrzeugen oder Personen entgegenzustehen. Dabei wird üblicherweise gegen Übersteigen, Untergraben, Entfernung und Durchdringen geschützt.

Mechanische Maßnahmen beschreiben die Anforderungen an Qualität und Ausprägung von Durchlässen in Mauer- oder Zaunanlagen zum Begehen oder Befahren: der höchste, festeste, mit Stachelbandkronen armierte Zaun und die massivste, höchste Mauer verlieren ihren Schutzwert, wenn die Türen und Tore, die ein Begehen bzw. Befahren der Perimeterschutzanlage ermöglichen, nicht dieselben Schutzmerkmale aufweisen, wie die gesamte Mauer- oder Zaunanlage: also gleiche Widerstandswerte, gleiche Höhe, gleiche Festigkeit und gleiche Armierung. Die sprichwörtliche Schranke (außer sie ist durch entsprechende personelle Sicherheitskräfte verstärkt) hat keinen sicherheitswirksamen Charakter, stellt lediglich eine Maßnahme der Zufahrtskontrolle (analog der Zutrittskontrolle) dar und bildet eine Sollbruchstelle im Zaunsystem. Insbesondere in Bezug auf Mauer- oder Zaunanlagen im Perimeter gilt der Grundsatz der Gleichwertigkeit von Sicherheits- und Schutzmaßnahmen: weisen Komponenten wie Durchgänge oder Durchfahrten Ungleichheiten in Bezug auf die restliche Umfriedungsqualität und -ausprägung bzw. die Widerstandswerte und -merkmale auf, ist die gesamte Umfriedungsanlage nur als so wirksam zu qualifizieren, wie die Komponente mit dem schlechtesten Widerstandswert. Das kennen wir

bereits vom Objektschutz: die Stahlbetonmauer mit einem Fenster ohne definiertem Widerstandswert ist in ihrer Gesamtheit nur so zu beurteilen, wie das rasch und einfach zu überwindende Fenster.

Unter **Elektronischen Sicherheitsmaßnahmen** wird – zumindest in Europa – landläufig die Detektion verstanden. In Teilen Afrikas und am amerikanischen Kontinent werden unter diesem Begriff häufig (auch) Elektrozaunanlagen verstanden, die dort weit verbreitet sind, die man in Europa jedoch maximal im Bereich militärischer Anlagen oder Anlagen der Kritischen Infrastruktur zu sehen bekommt, und das nur sehr vereinzelt. Wie im Bereich der Alarmtechnik im Gebäude ist die Forderung gestellt, dass unerwünschte Personen oder Fahrzeuge am Freigelände frühestmöglich zuverlässig detektiert werden, einen Alarm an eine ständig besetzte hilfeleistende Stelle übertragen und diese Stelle Interventionsmaßnahmen einleitet, die zum Ziel haben, den rechtswidrigen Aufenthalt am Gelände schnellstmöglich zu unterbinden. Unterschieden wird grob zwischen Detektion am Zaun, im Boden und über dem Boden: Zaundetektion hat das Ziel, ein Übersteigen, Unterkriechen oder Durchdringen des Zaunes zu detektieren, Bodendetektion erkennt im Wesentlichen Druckveränderungen durch Begehen oder Befahren armierter Flächen oder Korridore, die Detektion über dem Boden reicht von PIR-Meldern über Radar- und Mikrowellensensoren und Lasertechnik bis hin zur Videoanalyse.

Personelle Sicherheitsmaßnahmen

Die beste Armierung und Detektion bleiben wertlos, wenn nicht personelle Maßnahmen hinterlegt sind. Sicherheitskräfte können beispielsweise zur Kontrolle von Durchlässen in Mauern oder Zäunen herangezogen werden oder zu Kontrollen der Umfassungsintegrität, zwingend erforderlich sind Sicherheitskräfte jedoch als Interventionskräfte bei Detektion unerwünschter Personenanwesenheit.

Organisatorische Sicherheit

Wie immer im Bereich der Security bildet die Organisatorische Sicherheit einerseits die Basis für den Betrieb, stellt die Ressourcen zur Verfügung und gewährleistet andererseits durch Sicherstellung der Funktionalität und Angemessenheit i.S.e. Deming-Kreislaufes.

Im Hintergrund laufen – wie bei objektbezogenen Systemen auch – diverse Planungsgrundsätze wie das sogenannte Zwiebelschalenprinzip, das Prinzip „deter – detect – delay – deny – respond“, das Prinzip der Angemessenheit „soviel als nötig, so wenig als möglich“, usw.

Modelle

Spezifisch zugeschnitten auf den Schutz von Freigeländen existieren deutlich weniger Modelle, Normen und Literatur als zum Thema Objektsicherung. Ein praktikables Modell bieten **Kraheck-Zahn**[1] als Zonenkonzept für die Industrie, das – kleiner gedacht – aber durchaus nicht nur im industriellen Bereich anwendbar ist:

[1] Kraheck, A., Zahn, S. (2016). Grundlagen der Perimetersicherung. Berlin, Offenbach: VDE Verlag GmbH.

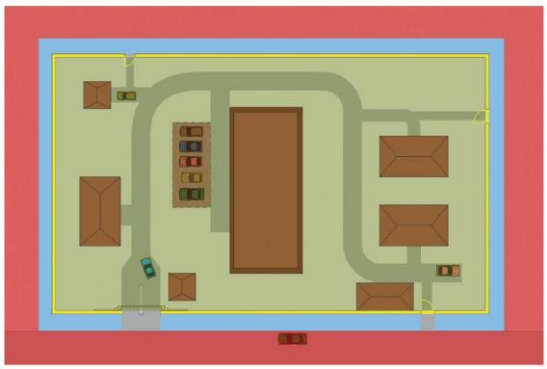

Abbildung 1 Quelle: Kraheck-Zahn: Grundlagen der Perimetersicherung

Zone 0 (rot) bezeichnet eine Grundfläche außerhalb des geschlossenen Perimeters, die NICHT in eigenem Eigentum steht und welches aus diesem Grund z.B. nicht videoüberwacht werden kann und auf welchem keine Befugnisse des Hausrechts ausgeübt werden können. Sehr wohl kann dieser Bereich aber in das Perimeterschutzkonzept bzw. das Sicherheitskonzept allgemein einbezogen werden, indem eine zulässige (also i.d.R. nicht technikunterstützte) Vorfeldbeobachtung stattfinden kann.

Zone 1 (blau) steht im Eigentum des Unternehmens, befindet sich aber AUSSERHALB des geschlossenen Perimeters. Optimalerweise definiert man hier an der Grenze zur roten Zone die juristische Grenze: diese zeigt (z.B. in Form eines Zaunes, der noch keinen sicherheitsrelevanten Anspruch erheben muss oder durch Beschilderung) deutlich an, dass ab hier ein Grundstück beginnt, auf welchem ein Besitzer sein Verfügungsrecht (= „Hausrecht“) ausübt. Dieser Bereich kann – da er im Eigentum des Unternehmens steht – auch technikunterstützt in das Überwachungskonzept eingebunden werden, beispielsweise durch Videoüberwachung, Videoanalyse oder Bodendetektion. Sinn derartiger Maßnahmen ist die frühzeitige Detektion unerwünschter Personenanwesenheit und dadurch die Gewährleistung frühzeitiger Interventionsmaßnahmen, um einen Angriff auf den geschlossenen Perimeter idealerweise noch vor dessen Realisierung beenden bzw. unterbinden zu können. Da das Grundstück im Eigentum des Unternehmens steht, sind in diesem Bereich bereits auch interventionelle Maßnahmen rechtlich zulässig, beispielsweise die Zurückweisung von Personen.

Zone 2 (gelb) definiert den geschlossenen Perimeter samt aller dazugehörigen Anlagen, also Mauern, Zäune, Mauer- und Zaundurchlässe etc. Der geschlossene Perimeter hat den Zweck, ein unerwünschtes Eindringen in das Unternehmensgelände zu verhindern und muss – anders als die Markierung der juristischen Grenze – den sich aus der Risikoanalyse ergebenden Überwindungsversuchen zumindest so lange standhalten, dass in Verbindung mit frühzeitiger Detektion Interventionskräfte so zeitgerecht herangeführt werden können, um ein rechtswidriges Eindringen auf das Gelände zu unterbinden. Findet eine Detektion nicht unmittelbar vor oder am Perimeter statt sondern erst innerhalb des geschlossenen Perimeters, sollen die baulichen Anlagen derart ausgestaltet sein, dass ein Überwinden für die sich aus der Risikoanalyse ergebenden Tätergruppen derart erschwert wird, dass es optimalerweise nicht zu einer Überwindung kommt und somit auch die Detektion nicht bemüht wird.

Zone 3 (oliv) definiert den Freigeländebereich auf eigenem Gelände und

Zone 4 (braun) bauliche Objekte.

Die deutsche **VdS 3143** definiert ebenfalls ein Zonenmodell:

Abbildung 2 Quelle: VdS 3143

Die **grünen Bereiche (Sektor 0)** definieren einen Bereich außerhalb des geschlossenen Perimeters, der überwacht werden kann, um Annäherungen an die Perimeterschutzanlage zu detektieren, wobei anders als bei Kraheck – Zahn nicht unterschieden wird, ob sich diese Zone in eigener oder fremder Verfügungsgewalt befindet und aufgrund der Besitz- bzw. Verfügungsverhältnisse die Möglichkeit der technischen Überwachung und Maßnahmenausübung besteht.

Der **blaue Bereich (Sektor 1)** stellt den geschlossenen Perimeter, also die Zaun- oder Maueranlage samt Duchlässen dar.

Gelb (Sektor 2) sind die unbebauten Flächen innerhalb des geschlossenen Perimeters dargestellt und

rot (Zone 3) die Gebäude am Gelände.

Intentionen des Perimeterschutzes

1st line of defence and detection

Die beiden zuvor vorgestellten Modelle (Kraheck-Zahn und VdS 3143) schützen den Perimeter vordergründig deshalb, um eine Annäherung an die eigentlich zu schützenden Gebäude (a) zu verhindern bzw. (b) so rechtzeitig zu detektieren, dass Interventionsmaßnahmen greifen können, bevor ein rechtswidriger Angriff bzw. Eindringversuch in die Gebäude stattfinden kann. Der Perimeter ist also die äußerste Zwiebelschale im Schutzsystem, die vorgelagerte Barriere, die die Aufgaben der deterrance und im Optimalfall auch der detection erfüllen soll. Eine ordentliche Barriere selektiert quasi weit vorgelagert potentielle Täter nach krimineller Energie und Fähigkeit und detektiert im Optimalfall jene, die versuchen, die Barriere zu überwinden; im weniger optimalen Fall erfolgt die Detektion erst NACHDEM die Barriere überwunden worden ist. Dazu aber später.

Der Perimeter stellt in dieser Konstellation die erste Verteidigungs- und Detektionslinie dar und hat Sinn und Ziel, Angriffe zu unterbinden, bevor Angreifer die eigentlichen Schutzobjekte, die baulichen Objekte, angreifen können: die Gebäudehülle würde dann bei entsprechender risikobasierter Ausprägung und Armierung und in Verbindung mit einer Einbruchmeldeanlage die „2nd line of defence and detection“ bilden, allfällig zu Schutzzwecken ausgeprägte und armierte Zonen im Objekt die „3rd line of defence“, ein allfälliges Werteschutzbehältnis, in welchem sich ein Schutzgut befindet, die „4th line of defence“ und die Interventionskräfte, die den rechtswidrigen Angriff beenden, eine weitere, letzte, Verteidigungslinie. Dem Prinzip „deter – detect – delay – deny – respond“ folgend würde am Zaun abgehalten und detektiert, durch die Überwindung der Freifläche bis zum baulichen Objekt und die bauliche Objekthülle selbst verzögert (weil es Zeit und Anstrengung bedarf, ins Objekt „einzubrechen“), durch das Wertschutzbehältnis der Angriff zurückgewiesen und durch Interventionskräfte würde der rechtswidrige Angriff unterbunden, also „beantwortet“.

1st and only line of defence

Gerade im Bereich des Perimeterschutzes existieren jedoch auch Risiken und Anwendungen, die die Sicherung und Detektion im Perimeter de facto zur ersten, aber auch (abgesehen von den Interventionkräften) einzigen Verteidigungslinie machen. Das ist immer dann der Fall, wenn sich zu schützende Güter gleichsam sofort hinter dem geschlossenen Perimeter im Freien befinden, also weitere Verteidigungslinien wie eine Gebäudehülle, weitere Zonierungen und Wertschutzbehältnisse nicht vorhanden sind. Als Beispiele dafür können Solarparks genannt werden (Ziel des Angriffes sind hier neben Sabotage Diebstähle von Solarpanelen, Kabeln und Wechselrichtern) oder Freilagerflächen, auf welchen wertvolle Rohstoffe gelagert sind, aber auch Ausstellungsflächen für Fahrzeuge und Geräte .... In all diesen Fällen befindet sich das Objekt der Begierde i.d.R. ohne weitere Schutz- bzw. Sicherungsmaßnahmen nahe hinter dem Zaun, wobei potenzielle Täter eine 2fache Aufgabenstellung bewältigen müssen: (a) wie gelangt man (möglichst ohne detektiert zu werden) auf das gesicherte Freigelände und (b) wie schafft man – wenn Diebstahl und nicht Sabotage die Motivation des Eindringens darstellt – das begehrte Gut aus dem umfriedeten Freigelände.

Da in diesem Fall de facto nur eine einzige Barriere (außer man würde ein mehrfaches Barrieresystem schaffen, wie dieses bei manchen militärischen Anlagen, Haftanstalten oder Grenzanlagen ... der Fall ist) Täter und Assets trennt, fordert diese hohe Aufmerksamkeit hinsichtlich der risikoangemessenen und -basierten Ausführung und Armierung. Da sich i.d.R. keine weiteren oder bedeutenden Verzögerungsfaktoren zwischen geschlossenem Perimeter und Asset befinden, muss die Detektion (a) so frühzeitig als möglich und (b) so zuverlässig als möglich erfolgen und müssen eine ggf. erste technikbasierte Täteransprache (über Lautsprecher, durch Beleuchtung, über Sirenen ...), die Alarmübertragung, die Alarmauswertung und -interpretation sowie das rasche Heranführen qualifizierter Interventionskräfte sichergestellt sein, um (großen) Schaden von Assets fernzuhalten, zumal derartige Freigelände i.d.R. personenfrei betrieben werden, also zumindest nachts, sonn- und feiertags keine Personen vor Ort sind.

Errichter von Perimeterschutz- und detektionstechnik

In Österreich dürfen bauliche und mechanische Barrieren von Inhabern einschlägig gültiger Gewerbeberechtigungen geplant und errichtet werden (Bauunternehmen, Metalltechniker, Schlosser ...), elektronische Detektionsmaßnahmen von Alarmanlagenerrichtern.

Die Hürden

Das System

Wie zuerst beschrieben sind Sicherheitssysteme im Objektschutz – setzt man eine Planung lege artis voraus! – immer als aufeinander abgestimmter Verbund baulicher, mechanischer, elektronischer, personeller und organisatorischer Maßnahmen zu verstehen. Eine singuläre Maßnahme stellt also KEIN Schutzsystem dar: ein einmal aufgestellter Zaun ohne Detektionsmaßnahmen und personelle Kontroll- und Interventionsmaßnahmen ... ist und bleibt ein Zaun und ist also noch lange kein „Sicherheitskonzept". Selbiges gilt für eine Detektion, die von einem unangemessenen Zaun begleitet wird und mit unzureichender Alarminterpretation und -

beantwortung auskommen muss: es handelt sich noch immer nicht um ein „Sicherheits- oder Schutzsystem“ und falls doch um ein schlechtes.

Was passiert also, wenn der Zaunbauer nach seiner Beurteilung und nach seinem Gutdünken einen Zaun aufstellt, der Alarmanlagenerrichter nach seiner Beurteilung und Idee eine Detektion plant und umsetzt, es der Alarmzentrale überlassen bleibt, wie Alarme zu interpretieren und wann/wie zu intervenieren ist und es dem Betreiber freigestellt ist, ob und wie er alles steuert und aufrechterhält? Man verlässt sich auf das Glück, dass alles irgendwie zusammenpasst und begibt sich sprichwörtlich – wie auf See und vor Gericht – in Gottes Hand. De facto geht es hier um das Außer-Acht-Lassen von Sorgfalt getragen von der Hoffnung, es werde schon passen und nichts passieren. Und diese Sorglosigkeit (hoffentlich nicht Inkompetenz) wäre allen an einem solchen Projekt Beteiligten vorzuwerfen. Vielleicht am wenigsten dem Betreiber derartiger Anlagen, denn von diesem ist kein einschlägiger Sachverstand vorauszusetzen, anders als bei den Errichtern der einzelnen sicherheitsrelevanten Gewerke.

Komplexe Systeme, wie Objektschutzsysteme – und somit auch Perimetrschutzsysteme, egal ob singulär oder im Konzept als 1st line of defence and detection“ – bedürfen eines Gesamtkonzeptes, einer Abstimmung, einer angemessenen Risikoherleitung und -beurteilung, Risikobehandlung, Planung, Umsetzung, Verortung in der Organisation und verschiedener Maßnahmen der Systemaufrechterhaltung. Hier ist der Sicherheitsplaner gefragt, der einem transparenten Prozess folgend die Risiken herleitet und errechnet, Stakeholderforderungen und Schnittstellen bearbeitet und einbezieht, einen angemessenen abgestimmten Maßnahmenverbund plant und die Maßnahmenumsetzung durch Experten begleitet und unterstützt.

Errichter

Während die Errichtung landschaftsbaulicher, baulicher und mechanischer Komponenten des Perimeterschutzsystems i.d.R. kaum Probleme bereiten und die Anforderungen nicht über den „normalen“ Sachverstand der jeweiligen Gewerbebetriebe hinausgehen (wobei es mit Sicherheit beispielsweise Zaunerrichter gibt, die auf Maschendrahtzäune um Einfamilienhäuser spezialisiert sind und welche, deren Expertise und Kompetenz in der Errichtung von Sicherheitszaunanlagen liegt; da muss man halt den richtigen Anbieter aussuchen), wird es bei der Errichtung der Detektionsmaßnahmen wesentlich schwieriger: jeder Alarmanlagenerrichter DARF Perimeterdetektion anbieten und beinahe JEDER Alarmanlagenerrichter bietet auch Perimeterdetektion an. Wie oft in der Alarmanlagentechnik kommen dann Systeme zum Einsatz, die vom Hersteller als „einfach zu montieren“ sowie „sicher und zuverlässig“ beschrieben werden und „keine besonderen (Vor)kenntnisse für Montage und Betrieb“ verlangen. Natürlich kann ein derartiges Out-of-the-box-System zu gebrauchen sein und seinen Nutzen haben, die Frage stellt sich hier aber nach Ort, Grund und Ziel des Einsatzes. Im kritischen Bereich, wo hohe Werte zu schützen sind, hohe Stakeholderanforderungen zu erfüllen sind, die Abwälzung des (Rest)risikos eine hohe Rolle spielt … ist von derartigen Errichtern und Lösungen abzuraten: hier bedarf es einerseits hoher Spezialisierung des Errichters und der richtigen Auswahl von Detektionsart und

Produkten/Komponenten. Warum? Anders als bei der Errichtung von Einbruchmeldeanlagen findet die Detektion im Freien statt: je nach Einsatzgebiet bei extremen Temperaturen und Temperaturschwankungen, unterschiedlichen Wetter- und Witterungsbedingungen, unterschiedlichen Bodenverhältnissen ... All diese Umstände verlangen eine entsprechende Beurteilung und Erfahrung alleine die Auswahl der möglichen Detektionsvarianten betreffend und dann jene der passenden Hersteller bzw. Produkte. Dazu kommt die Justierung und Kalibrierung der verbauten Technik: schließlich sollen bei allen vor Ort denkbaren Sicht- und Wetterverhältnissen 24/7/365 zuverlässige Detektionen ungewünschter Personenanwesenheit erfolgen und dabei die Fehl- und Falschalarmauslösung so gering wie möglich gehalten werden. All das ist hoch aufwendig und verlangt nach hoher Expertise und Erfahrung. Wirklich erstklassige Errichter von Perimeterdetektion verlassen sich längst nicht mehr auf Produktbeschreibungen von Herstellern, sondern betreiben auf eigenen Testgeländen Versuche und Auswertungen einer Vielzahl unterschiedlicher Anlagen, Systeme und Hersteller, um für jede Kundenanforderung, jede(s) Spezifikum, Wetter, Bodenbeschaffenheit etc. die richtige Lösung anbieten zu können, immer unter der Prämisse der zuverlässigen Detektion bei möglichst geringer Fehlerquote. Bezogen auf den österreichischen Markt ist uns EIN einziges Unternehmen bekannt, das sich vorwiegend auf Perimeterdetektion spezialisiert hat, diesbezüglich auch weltweit tätig ist und ein eigenes Testgelände betreibt, auf welchem 24/7/365 verschiedene Produkte und Einstellungen in den Bereichen Videoanalyse, Zaundetektion und Bodendetektion getestet werden. Regelmäßig erfolgen für das Unternehmen auf diesem Testgelände auch Überwindungsversuche durch unabhängige Sachverständige.

Komponenten

Ebenfalls anders als in der Indoor-Alarmtechnik ist die Zahl der Hersteller von Perimeterdetektion überschaubar. Hier gilt es beispielsweise in der Videoanalyse die – bezogen auf die Verhältnisse und Angriffsszenarien – passende Kamera für den jeweiligen Einsatzort mit der passenden Analysetechnik zu verbinden. Setzt man Detektion im Boden ein, wird es ohne Bodenerkundung nicht gehen, da unterschiedliche Bodenverhältnisse, Bodendichten und nicht zuletzt die Möglichkeit, die Sensorik durchgehend in einer gewissen Tiefe zu verlegen, vor der Planung feststehen müssen, denn einerseits ist die Frage zu stellen, ob man an der entsprechenden Örtlichkeit die Detektionsform überhaupt verwenden kann und andererseits welche Produkte anbetrachts der Möglichkeiten und Bedingungen vor Ort die besten Ergebnisse erzielen werden. Die Methode einer Zaundetektion, und ob eine solche überhaupt möglich ist, hängt nicht nur von der Qualität des Zaunes an sich, sondern auch vom Gelände ab. Wählt man eine Detektion über dem Boden, beispielsweise mittels PIP, Radar oder Mikrowelle, sind die hersteller- und produktspezifischen Detektionswinkel bzw. -kegel anbetrachts der Zaun- und Geländegegebenheiten zu überprüfen etc.

Allgemeine Überlegungen zur Planung

Die OVE-Richtlinie R 2 + AV:2017 fordert in Bezug auf Einbruch- und Überfallmeldeanlagen, dass sie „vorzugsweise so zu konzipieren sind, dass Einbrüche bzw. Einbruchversuche möglichst frühzeitig erkannt und gemeldet werden, wobei

mechanische Sicherungseinrichtungen und die Überwachung durch die EMA unter Berücksichtigung der voraussichtlichen Interventionszeit so aufeinander abgestimmt werden, dass die Interventionskräfte nach Eintreffen einer Meldung den Einsatzort möglichst schon erreichen können, bevor der Täter die mechanischen Sicherungseinrichtungen überwunden hat ...".

Vorweg kann einmal gesagt werden, dass mit Sicherheit mehr als 95% aller Einbruchmeldeanlagen so konzipiert sind, dass Alarm erst ausgelöst wird, wenn die mechanischen Sicherheitseinrichtungen (Fenster, Türen ...) bereits überwunden worden sind. Das hat weitreichende Folgen: bei Alarmauslösung ist der Täter bereits im Objekt und verkürzt dadurch die – sollte sie überhaupt berücksichtigt worden sein und falls ja richtig berechnet – den Interventionskräften zur Verfügung stehende Zeit, um den rechtswidrigen Angriff rechtzeitig vor Erreichung des Täterzieles zu beenden.

Zurückkommend auf die Perimetersicherung ist die Forderung, die für Einbruchmeldetechnik im Objektinneren gilt, von der Logik her auch hier zu stellen: Die Umfriedung eines Freigeländes ist mit einer Detektion verknüpft, wobei der Angriff auf die Grundstücksumfassung so rechtzeitig detektiert wird, dass eine Angriffbeendigung durch Interventionskräfte noch VOR Überwindung der Mauer- bzw. Zaunanlage erfolgen kann. Salopp gesagt ist das mit einer entsprechenden Detektion AM Zaun bei entsprechender Zaunausgestaltung möglich und ggf. mit Videoanalyse, wenn man deren Detektion zumindest teilweise VOR den umfriedeten Perimeter legt bzw. dort bereits zu detektieren beginnt. Ebenso salopp gesagt wird eine derartige Kameraeinstellung in der Videoanalyse die Falschalarmquote erhöhen, denn jeder, der sich dem Zaun nähert, hat vermutlich nicht auch die Absicht, ihn zu überwinden, wird jedoch detektiert. Eine weitere Möglichkeit bestünde z.B. in einer In- oder Über-Bodendetektion in der Zone 1 des Kraheck-Zahn-Modells, also auf eigenem Grund AUSSERHALB des geschlossenen Perimeters. Das würde aber grob gesagt bedingen, dass die juristische Grenze bereits so ausgestaltet ist, dass zu deren Überwindung eine Absicht vorausgesetzt werden kann (das führt zu einem zweiteiligen Zaunsystem mit einem dazwischenliegenden Korridor, in welchem die Detektion untergebracht ist) und der Korridor zwischen den beiden Zäunen (wobei der äußere nicht die Sicherheitsqualität des inneren haben müsste) ausreichend breit ist, um nicht unter Zuhilfenahme einfacher technischer Mittel überwunden werden zu können, um die Detektion zu umgehen.

In der Praxis – wendet man weder das Korridormodell noch Zaundetektion an – vertraut man darauf, dass Täter die Zaunanlage nicht überwinden können oder von sichtbaren Sicherheitseinrichtungen abgeschreckt werden, da sie hohes Entdeckungs- und Identifikationsrisiko befürchten müssen und detektiert insbesondere aus Gründen der Geringhaltung von Falschalarmen erst so früh als möglich NACH Überwindung des geschlossenen Perimeters. Das heißt, die Interventionsmaßnahmen beginnen erst dann, wenn sich Personen bereits unautorisiert am Gelände aufhalten. Es wurde also der Anspruch aufgegeben, Täter gar nicht erst auf das Gelände und somit zu Assets vordringen zu lassen, sondern Angriffe bereits AUSSERHALB des Perimeters zu beenden.

Nun mag das eine untergeordnete Rolle spielen, wenn Perimeterschutz und -detektion Teil eines umfassenden Sicherheitskonzeptes sind, welches den Schutz von Assets IN Gebäuden auf einem perimetergesicherten Gelände zum Ziel hat. Da muss noch eine bauliche Außenhaut überwunden werden etc. Wenn aber bei einem solchen System auch „Sabotage" oder „Sachbeschädigung" in der Risikoanalyse aufpopen, ist die Detektion erst NACH dem geschlossenen Perimeter zweimal zu überdenken.

Befinden sich zu schützende Assets -. auch unter dem Aspekt des Diebstahles - auf Freigeländen wie bei Solarparks, Umspannwerken, Kraftwerken, Freilagerplätzen etc. ist die Detektion erst NACH Zaunüberwindung ebenfalls äußerst kritisch zu betrachten: es wird bewusst das Risiko eingegangen, den/die Täter erst einmal auf das Gelände zu lassen und somit die Gefahr, dass dort auch Schaden bis zur Intervention verursacht wird. Eigentlich fatal. Denn wenn Interventionskräfte nicht vor Ort präsent und entsprechend qualifiziert sind, sondern nach Alarmübertragung und hoffentlich richtiger Interpretation erst herangeführt werden müssen, vergehen nicht selten mehr als 30 Minuten (die Berechnung/Herleitung der Interventionszeit wird Thema eines anderen Papers sein). Und in 30 Minuten kann viel geschehen, insbesondere im Sabotagebereich, aber auch im Diebstahlbereich.

Gerade wenn Assets auf Freigeländen zu schützen sind und eine Zaun- oder Maueranlage nicht nur die erste sondern auch die einzige Verteidigungslinie darstellt und die Perimeterdetektion die erste aber auch einzige Detektionslinie ist, wäre es wünschenswert, der Normforderung zu entsprechen: (1) eine Detektion erfolgt so frühzeitig wie möglich AUSSERHALB der geschlossenen Perimeterumfassung, (2) diese ist derart gebaut und armiert, dass sie den/die Täter am Eindringen auf das Gelände solange hindert, bis Interventionskräfte innerhalb der berechneten Maximalinterventionszeit den Angriff noch außerhalb des geschützten Geländes unterbinden können.

Oftmals wird versucht, Schaden von Assets auf Freigeländen abzuwenden, indem die Detektion NACH Überwinden einer Zaun- oder Maueranlage Maßnahmen auslöst, die den Täter erkennen lassen, dass er detektiert wurde, beispielsweise die Flutung des Geländes mit Weißlicht, um den Täter sozusagen sichtbar zu machen, ihn „in die Auslage zu stellen", das Angehen von Sirenen, um die anonyme Öffentlichkeit zu alarmieren und den Täter ebenso unter Druck zu setzen wie bei der Lichtflutung, die Täteransprache über Lautsprecher, um zu zeigen, dass eine Entdeckung stattgefunden hat und eine Intervention eingeleitet worden ist …

Im Vergleich zur Gestaltungsvariante der Angriffsunterbindung noch AUSSERHALB des Zaunes geht mit der Detektion INNERHALB des Perimeters – auch bei mit der Detektion gekoppelten Maßnahmen, die dem Täter die Tatsache der Detektion vor Augen führen und ihn zur Aufgabe seines Vorhabens und zur Flucht bewegen sollen – IMMER zwangsläufig einher, dass ein Risiko – in welcher Ausprägung auch immer – in Kauf genommen wird. Dieses mögliche Risiko bzw. das mögliche Schadenausmaß ist (a) den Kosten einer frühzeitigen Detektion außerhalb des geschlossenen Perimeters gegenüberzustellen und (b) jedenfalls daraufhin zu überprüfen, ob es vollumfänglich z.B. im Wege von Versicherungen abgewälzt ist.

Fazit

Schutz- und Sicherungsmaßnahmen im Perimeter sind nicht einfach „eine Alarmanlage draußen", sondern entweder wichtiger Teil eines Gesamtschutzsystems oder alleinige Komponente des Schutzes von Assets im Freien. Perimetersicherungsmaßnahmen bestehen - wie alle Objektschutzsysteme – aus einem risikobasierten, abgestimmten Miteinander von baulichen, mechanischen, elektronischen, personellen und organisatorischen Maßnahmen und verfolgen die Abschreckung, Abhaltung, Verzögerung und letztlich Zurückweisung und Beendigung von Angriffen. Da sämtliche Komponenten Witterungseinflüssen ausgesetzt sind und der Anspruch der Detektion i.d.R. 24/7/365 besteht, sind an den Errichter insbesondere der Perimeterdetektion extrem hohe Anforderungen hinsichtlich Fach- und Produktkenntnis sowie Erfahrung gestellt, da neben Witterungsbedingungen i.d.R. auch Boden- und Geländebedingungen und -beschaffenheiten großen Einfluss auf die Möglichkeit der Maßnahmengestaltung und -effizienz haben. Aufgrund des Umstandes der Detektion im Freien ist mit einer höheren Fehl- und Falschalarmquote zu rechnen als bei Indoor-Alarmanlagen, denn nicht nur Regen, Schneefall, Schneedecke, Temperaturunterschiede, Sonnen- und sonstige Lichteinflüsse ... sondern auch Bewuchs und Tiere im überwachten Bereich können zu unerwünschten Alarmauslösungen oder aber auch Nicht-Auslösungen führen. Aufgrund der enormen Fremdeinflussausetzung derartiger Freigeländedetektionssysteme ist jedenfalls eine Detektionsredundanz anzuraten, sodass 2 unterschiedliche Detektionssysteme in einer Oder-Verknüpfung zusammenwirken: eines der beiden muss unerlaubte Personenanwesenheit im Überwachungsbereich – besser Überwindungsversuche des geschlossenen Perimeters - jedenfalls detektieren und die Interventionskette auslösen. Probate Kombinationen sind beispielsweise Videoanalyse und Bodendetektion oder Zaundetektion, Detektion am Zaun und Detektion über dem Boden etc. Abzuraten ist jedenfalls von einer Und-Verknüpfung zur Reduktion von Falschalarmen; was im Innenbereich relativ sicher ist, begünstigt im Außenbereich überproportional das Unterbleiben gewünschter Detektion.

Ist das System nicht derart aufgebaut, dass eine zuverlässige Detektion bereits außerhalb eines geschlossenen Perimeters erfolgt und entsprechend auf die errechneten Risiken und Szenarien ausgelegte und armierte Mauer-/Zaunanlagen ein Eindringen auf das geschützte Freigelände verhindern, nimmt man zwangsläufig in Kauf, dass unautorisierte Personen auf das Grundstück gelangen, verkürzt die Aktionszeit der Interventionskräfte, erschwert die Intervention und Angriffsunterbindung und nimmt damit Risiken von – je nach Ergebnis der Risikoanalyse – Sabotage, Beschädigung oder Diebstahl in Kauf, deren vollumfängliche Abwälzung z.B. im Wege einer Versicherung einer genauen Überprüfung bedarf.

Die Autoren:

Mario Trutzenberger, ist selbstständiger Sicherheitsberater für Physical Security, Notfall- und Krisenmanagement und Materiellen Geheimschutz und modulverantwortlicher Lektor

für Physische Sicherheit im Fachbereich Risiko- und Sicherheitsmanagement an der FH Campus Wien.

Sandro M. Trutzenberger ist Absolvent des Bachelorstudiums Integriertes Sicherheits-Management, Student im Masterstudium Public Management und Security-Consultant mit Schwerpunkten Security-Risc-Analysis und Physical Security.

Näheres unter https://secfirm.at.